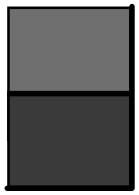


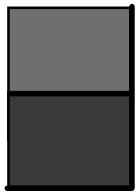
# An Intermediate System's View of IPSEC

Cheryl Madson

Senior Software Engineer

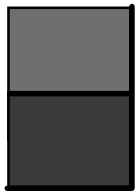
IOS Security

Cisco Systems



# Agenda

- An overview of ISAKMP, Oakley and IKE
- The view of IPSEC from an intermediate system (e.g. router or firewall)

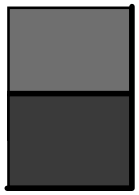


# ISAKMP, Oakley and IKE

CISCO SYSTEMS

# ISAKMP, Oakley and IKE

- ISAKMP: Internet Security Association and Key Management Protocol
  - Provides a framework for establishing shared security policy and deriving keying material
    - Supports various key generation mechanisms, ex. Oakley
    - Supports various authentication mechanisms
    - Domains of Interpretation, ex. IPSEC
- Oakley
  - Key generation mechanism used with IPSEC



# ISAKMP, Oakley and IKE

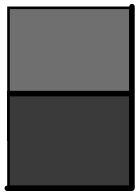
- IKE: Internet Key Exchange
  - Formerly known as “the resolution document”
  - Specifies “profile” for applying ISAKMP and Oakley within the context of IPSEC

# General ISAKMP Concepts

- ISAKMP “daemons” on the IPSEC peers establish a protected pipe between themselves (main mode).
  - Peers identify themselves, prove themselves to each other, using such mechanisms as
    - pre-shared secrets
    - certificates w/RSA-signatures
    - certificates w/RSA-encryption (encrypted nonces)
  - Authenticated entities derive a shared secret
  - Main Mode identifiers are “blobs” to identify the ISAKMP peers such as IP address, DNS name, DN name

# General ISAKMP Concepts

- Session keys and corresponding policy is established using Quick Mode exchanges
  - negotiation of set of security transforms
  - specification the endpoints on whose behalf the security association bundle is being established
    - Source address/subnet, address range
    - Destination address/subnet, address range
    - Protocol
    - Source/destination port (no ranges)
  - derivation of keys for use in data protection



# The IPSEC View from an Intermediate System

# Mobile User to Firewall

Single (mobile) user interacting with firewall to gain access to the corporate network

- Interaction to establish an IPSEC-protected pipe between client and firewall
- Providing at least authentication/integrity services, possibly also confidentiality services

# Mobile User to Firewall

- SA granularity usually pinned down to an individual session, if not host-to-host or host-to-subnet
  - finer-grained SAs can provide input for finer-grained policy decisions
  - fine granularity can quickly consume resources; more state and key management
- Issues of identity
  - secure delivery of DHCP
  - allowing “dynamically obtained” IP address to be used as on-the-fly identification of remote client

# Intemediate System Tunnels

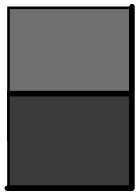
IPSEC-protected tunnels between intermediate systems

- Commonly providing both confidentiality and authentication/integrity services
- SA granularity usually subnet-to-subnet basis
  - scaling in terms of state management
  - coarser-grained SAs can provide a limited level of protection against traffic analysis
- IP identities usually known in advance; can predefine identity-based policy

# Data Flows

An intermediate system works from the view of "data flows" as opposed to individual sockets

- security transformations applied to flow
  - no concept of socket: no socket_open() with "apply security against socket now"
    - router does not know when an individual (end system) session begins or ends; fine-grained SA lifetime may exceed actual socket lifetime
    - similar issues with dynamic Network Address Translation
      - should link fine-grained SA lifetimes with other dynamic lifetimes; this linking can add to challenge



# Data Flows

- SAs at the session level may cause router to reassemble datagrams to select the correct SA; represents a processing hit

Routers have a definite preference for “big fat pipes”

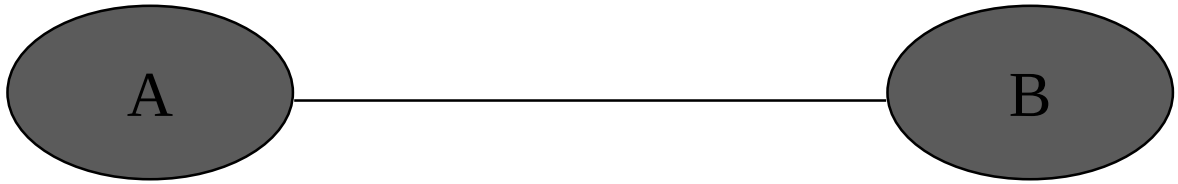
CISCO SYSTEMS

# Identity Confusion

- Quick mode IDs determine the identity of the traffic allowed in this tunnel
  - Source address/subnet, address range
  - Destination address/subnet, address range
  - Protocol
  - Source/destination port (no ranges)
  - No “lists” of quick mode IDs; no passing of ACLs
  - Quick mode IDs used as “selector” by sender, “filter” by receiver

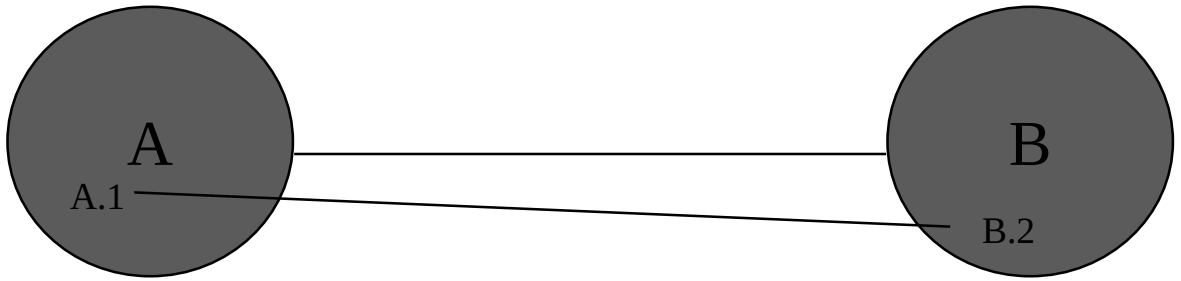
# Identity Confusion

- For a granularity greater than an individual session, need to determine how to represent a possibly complex policy rule to the peer to ensure selection of correct “pipe”
  - simple: all traffic from subnet A to subnet B is accepted in this IPSEC tunnel and shall be encrypted



# Identity Confusion

– more complex: one tunnel for traffic from subnet A to subnet B; EXCEPT traffic from host A.1 to host B.2




- Ideal would be that sender not even send traffic that the receiver would then turn around and drop on the floor
- Ordering of selectors (e.g. ACLs) doesn't help if peers have different ordering
- Punt Quick Mode IDs altogether?

# Fault Tolerance and Redundancy

- In a flow-based security mechanism with primarily one-way flows, how does sender know that receiver has died/restarted?
  - may wish to fall back to an alternate receiver or alternate path
  - very short SA lifetimes can be a short term solution -- forcing frequent ISAKMP exchanges as a form of peer liveness check
  - a future tunnel discovery mechanism can assist in solving this problem